UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Google Accounts associated with earlcunningham90@gmail.com and byrdthroop@gmail.com

Case No. 20 MJ 240

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 United States Code, Section 111	Assaulting a Federal Employee

The application is based on these facts:

See attached affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days *(give exact ending date if more than 30 days:*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

USPIS Postal Inspector Scott Zimmerman
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: November 18, 2020

Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Inspector Scott Zimmerman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC (hereafter "Google") to disclose to the government records and other information, including the contents of communications, associated with the Google Accounts earlcunningham90@gmail.com and byrdthroop@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Postal Inspector with the United States Postal Inspection Service, (USPIS), and have been so employed for approximately 3 ½ years. The USPIS is the primary investigative arm of the United States Postal Service (USPS) and is charged under Title 18, United States Code, 3061 with the enforcement of laws governing the use and movement of the United States Mail, violent crimes, narcotics trafficking and identity theft involving the United States Mail. My current responsibilities include the investigation of criminal investigations involving shootings, robberies, burglaries and assaults. Previously, I was a Federal Air Marshal for approximately 10 ½ years.

3. Throughout my employment as an U.S. Postal Inspector, I have participated in the execution of search warrants involving searches and seizures of residences, businesses, and vehicles. These warrants often included seizure of computers, cellular phones, related electronic equipment such as printers and laminators and requisite software to operate computers and

peripheral devices. I have participated in numerous complex narcotics, shootings, armed robbery, burglary and assault investigations in violation of Title 18, United States Code, Sections 924(c), 2114, 2115, 111 and other related offenses.

4. The factual allegations set forth herein are based on my personal observations and knowledge, in addition to information obtained from other investigators, public and private records, cooperating witnesses and other involved parties and sources as indicated herein. Because this Affidavit is submitted for the limited purpose of demonstrating probable cause for the warrant sought, I have not included each and every fact known to me or other law enforcement officers about this investigation.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that "**Suspect 1"** has committed a violation of 18 U.S.C § 111 (assaulting a federal employee). Further, there is probable cause to search the information described in Attachment A for evidence of this crime, as described in Attachment B. The court has jurisdiction to issue the proposed warrant because it is a, "court of competent jurisdiction," as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

JURISDICTION

6. The Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On August 31, 2020, the USPIS followed up on a report of an USPS carrier being assaulted in Kenosha, WI 53140. USPS carrier, "Victim 1," was physically attacked while conducting USPS duties. I, Inspector Zimmerman, was advised Victim 1 was hearing impaired and could be reached via phone. The Kenosha Police Department (KPD) responded to the scene.

8. On August 31, 2020, at approximately 3:30 PM, Central Standard Time (CST), Victim 1 was delivering mail on USPS, Route 4070, in Kenosha, WI on the 2200 block of 53rd street in Kenosha, when he was attacked. KPD responded to the 2200 block of 53rd street in Kenosha, WI in regards to a reported assault on a mail carrier. KPD explained Victim 1 sustained bruising behind the right ear; marks on his neck and scratches on his face. KPD said when they arrived on scene, Victim 1 had blood on his hands as well.

9. On September 1, 2020, I interviewed Victim 1. Victim 1 said his normal delivery route is Route 35, but he was covering Route 70 when he was assaulted. Victim 1 said the assault occurred on the 2200 block of 53rd St. Kenosha, WI, 53140 at approximately 3:30 PM CST. Victim 1 said he saw a small group of people gathered on the street. Victim 1 thought the group of people may have been talking about him, because they were looking at him. Victim 1 advised Suspect 1, who eventually attacked him, took his picture with a cell phone.

10. Victim 1 described Suspect 1 as an African American Male standing approximately 5'7 to 5'8 feet tall weighing approximately 180 pounds. Victim 1 said Suspect 1 was wearing a white tank top, did not have a hat on, but had a mildly shaved head. Victim 1 stated Suspect 1 may have had a tattoo on the left side of his face, but did not remember seeing any other distinguishing features.

11. Victim 1 explained that Suspect 1 approached him and accused him of hitting Suspect 1's car. Victim 1 stated he told Suspect 1 he did not hit his car, because he was nowhere near a car. Victim 1 said Suspect 1 repeatedly asked him for an ID. Victim 1 advised he walked away and stated it was then Suspect 1 attacked him from behind. Victim 1 explained Suspect 1 struck him multiple times, specifically in the face, neck and behind the ear. Victim 1 advised there was only one suspect who attacked him. Victim 1 said one of his $5000.00 hearing aids was damaged during the assault.

12. Following the assault, Victim 1 said he recovered and walked away. Victim 1 indicated Suspect 1 did not brandish a weapon during the assault. Victim 1 stated Suspect 1 did not take anything from him, including the mail. Victim 1 indicated he immediately called his supervisor to inform him of the assault. The supervisor reported the assault to KPD, who responded to the scene. Prior to the assault, Victim 1 stated he had never seen nor did he know Suspect 1 or any of the people in the small group in question.

13. On September 3, 2020, Inspectors notified KPD they were in the area and would begin a soft surveillance and canvass for cameras on 53rd Street Kenosha, WI 53140 between 22nd and 23rd Avenues where the assault reportedly took place. Inspectors began conducting a soft surveillance of the neighborhood where Victim 1 was physically assaulted on August 31, 2020 at approximately 3:30 PM CST. Inspectors saw a group of approximately 10 people sitting in front of 2215 53rd St. Kenosha, WI 53140, reportedly near where the assault took place. Inspectors did not find any cameras on the houses or businesses located on 53rd Street between 22nd and 23rd avenues.

14. Inspectors met with Victim 1 for a follow up interview at 1073 Sheridan Rd. Kenosha, WI 53140, while he was conducting USPS duties on his route. Victim 1 provided more

specifics on his location when he was assaulted on August 31, 2020. Victim 1 stated he was on his first loop of the route, walking East on 53rd Street in Kenosha, WI 53140, towards 22nd Avenue when he was assaulted. Victim 1 gave an approximate location near 2215 53rd St. and 2219 53rd street as to where the assault took place.

15. Victim 1 reiterated that Suspect 1 had a tattoo or a possible scar on the left side of his face. Victim 1 recalled the vehicle Suspect 1 got into following the assault was an older model Mercedes Benz SUV, silver in color. Prior to the assault, Victim 1 recalled Suspect 1 pointing out damage to the passenger side bumper specifically below the headlight. Victim 1 described the damage as a piece of the bumper being loose. Victim 1 said there were scratches on the bumper as well. Victim 1 stated Suspect 1 was blaming Victim 1 for the damage. Victim 1 said his USPS vehicle was not on the same block as Suspect 1's car. Victim 1 advised when he walked away from Suspect 1, he was attacked.

16. Following the meeting with Victim 1, Inspectors resumed a soft surveillance on 53rd Street Kenosha, WI 53140 between 22nd and 23rd Avenues in search of a Silver Mercedes SUV. Inspectors identified a Silver Mercedes SUV sitting in the driveway of 2215 53rd St. Kenosha, WI 53140. Inspectors identified the Wisconsin license plate as AGR-9249. The vehicle was not parked in the driveway earlier in the surveillance.

17. I called the National Law Enforcement Communications Center (NLECC) and requested a license plate query. According to NLECC, WI license plate AGR-9249 was not registered to a Silver Mercedes SUV. Shortly thereafter, the suspect vehicle departed 2215 53rd St. Kenosha, WI 53140 and headed south bound on 22nd Avenue Kenosha, WI. Inspectors immediately notified KPD of the situation. Due to a last minute visit by then-Presidential

Candidate Joe Biden and concerns over violent protesting and rioting, the KPD was unable to provide a squad car for immediate response.

18. Considering the totality of the circumstances, Inspectors conducted a controlled vehicle stop of the Silver Mercedes Benz GL430, WI License Plate AGR-9249, on 22nd Ave and 63rd St. Kenosha, WI 53140 just west of the Uptown Brass Center. This location was a couple of blocks from potentially violent protests and rioting. Inspectors ensured the vehicle was pulled over in the most safe and tactically advantageous area under the capricious circumstances. Large crowds began to gather during the vehicle stop on 22nd Ave. west of where the vehicle was pulled over.

19. Inspectors approached the Silver Mercedes Benz GL430, Wisconsin License Plate AGR-9249. I identified myself verbally while presenting my USPIS credentials to the driver. I immediately noticed a tattoo below the left eye of driver. This was a distinguishing feature Victim 1 provided in his description of Suspect 1 during interviews. I subsequently requested the driver's identification. The driver provided me with his Wisconsin Driver's License. Suspect 1's identity was revealed and I took Suspect 1's photo.

20. During the stop, Suspect 1 denied having any knowledge regarding Victim 1 being assaulted on August 31, 2020. Suspect 1 denied being on 53rd St. Kenosha, WI 53140 during the time of the assault. Suspect 1 said he heard about the carrier being attacked after it had happened, but could not identify who told him about the assault. Suspect 1 said he was at his "Baby Mama's house," during the time of the assault. Suspect 1 did not make eye contact with me when asked about the assault. Suspect 1 insisted he was currently on his way to the hospital, because his "Baby Mama" was having a high risk pregnancy and she may be giving birth. Suspect 1 could not identify what hospital he was driving to. Suspect 1 again denied taking part in or having any knowledge of the assault on Victim 1, stating, "that's just stupid to attack a mailman."

21. Suspect 1 was made aware the license plate on the Mercedes Benz GL 430 he was driving did not match the vehicle to which it was registered. Suspect 1 stated he was aware the license plate was switched and advised it was registered to a Red Dodge Avenger that belonged to his wife. This vehicle information was corroborated with the NLECC driver's license query for Wisconsin license plate AGR-9249.

22. During the stop, I took pictures of the bumper on the Mercedes Benz Model GDL 430 Suspect 1 was driving. The photos illustrate scratches on the right side bumper and a loose bumper on the passenger side of the vehicle. This damage was similar to the damage described by Victim 1 during the follow up interview shortly before the controlled vehicle stop.

23. I sent the photo of Suspect 1 to Victim 1 to inquire if Suspect 1 was involved with the assault. Victim 1 immediately responded by text message, identifying Suspect 1 as the man who assaulted him and took his picture.

24. KPD arrived on scene. Inspectors informed the officers Suspect 1 was driving a vehicle with a license plate which did not match the registration of the vehicle. Inspectors further explained how Victim 1 identified Suspect 1 as the man who assaulted him from a photo sent to Victim 1 a few minutes prior.

25. KPD advised Suspect 1 is currently on parole. The responding KPD Officers were abruptly called to an emergent situation, and Suspect 1 was free to leave.

26. On September 15, 2020, I spoke with Suspect 1's WI State Parole Officer. The parole officer provided phone number 773-297-7025 as the contact number she had on file for Suspect 1. The parole officer stated Suspect 1 is not on electric monitoring. I asked if the parole officer would be able to search the pictures on Suspect 1's phone during her next meeting with him. The parole officer stated, because of the COVID-19 pandemic she is restricted from making

contact with parolees unless it was emergent. The parole officer said she would put in a request with her management to see if she would be able to arrange a meeting with Suspect 1 to look at the pictures on his phone.

27. On September 29, 2020, I was informed that KPD received a tip from a caller, "Witness 1." Witness 1 left a message stating she "knows" who battered the postal worker. KPD attempted to call Witness 1 back, but was unsuccessful.

28. On October 8, 2020, Inspectors interviewed Witness 1, who indicated Suspect 1 drove to her current residence at, 4722 36th Ave. Kenosha, WI 53144 in the late afternoon or early evening on August 31, 2020. Witness 1 said Suspect 1 was drunk when he arrived. Witness 1 stated Suspect 1 told her he assaulted a postal worker on 53rd Street, Kenosha, WI 53140. Witness 1 said she knew the assault occurred on August 31, 2020, because it was Suspect 1's birthday. Suspect 1's date of birth was corroborated by his WI Driver's License and the National Crime Information Center (NCIC).

29. Suspect 1 told Witness 1 the postal worker bumped into Suspect 1's vehicle with his mail bag. Suspect 1 told Witness 1 he confronted the postal worker and asked the postal worker if he was going to pay for his front bumper. Suspect 1 told Witness 1 the postal worker did not engage in the confrontation and walked away from Suspect 1. Suspect 1 told Witness 1 he felt disrespected when the postal worker walked away from him, so he went after the postal worker. Suspect 1 stated to Witness 1, "I knocked out a postal worker." Witness 1 reiterated Suspect 1's statement multiple times during the interview.

30. Witness 1 said that Suspect 1 took a picture of the postal worker with his phone, around the time of the assault. Witness 1 believed the photo would probably still be on Suspect 1's phone. Witness 1 said Suspect 1 showed her the photo he took of the postal worker he assaulted.

Witness 1 described the postal worker in the photo as a white male with short hair. Witness 1 stated the postal worker in the photo had a blue shirt on and wore sunglasses. Witness 1 said that if she saw a picture of the postal worker, she would be able to identify him. Witness 1 said she did not know the postal worker in the photo on Suspect 1's phone.

31. Witness 1 explained she gave birth to a baby girl on October 6, 2020, and Suspect 1 was the father of the child. Witness 1 explained she is no long together with Suspect 1, but they did live together at 5305 52nd St. #2 Kenosha, WI 53140 for a short time. Witness 1 did not believe Suspect 1 still resides at this address and now lives in a house on 53rd St. Kenosha, WI 53140, near the location of the assault.

32. Witness 1 stated Suspect 1 no longer drives the Mercedes SUV he had been driving at the time of the assault, and now drives a maroon Chevy Malibu with tinted windows. Witness 1 stated Suspect 1 is physically and verbally abusive towards her.

33. Witness 1 adamantly stated she would assist Inspectors any way she could and did not want to harbor a fugitive. Witness 1 volunteered to take Inspectors to the exact location where she believes Suspect 1 is currently residing. Witness 1 provided phone number 773-297-7025 as the most current cell phone number for Suspect 1.

34. On October 26, 2020, I followed up with Suspect 1's WI State Probation Officer and requested that the probation officer set up a meeting with Suspect 1 for October 27, 2020. Suspect 1's probation officer spoke with her supervisor and stated she would attempt to set up an in-person meeting with Suspect 1 at her office located at 4911 88th Ave. Kenosha, WI 53144 at 1:00 PM on October 27, 2020. The objective of the meeting was to execute a Wisconsin Act 79 search for Suspect 1's phone.

35. On October 27, 2020, Suspect 1 reported to the WI State Probation Office located at 4911 88th Ave. Kenosha, WI 53144. Upon Suspect 1's arrival, I, in coordination with the probation officer, executed a Wisconsin Act 79 search for Suspect 1's phone. Suspect 1 handed over his cell phone and passcode without incident. The phone was put into airplane mode and immediately transported to North Central High Intensity Drug Trafficking Areas (HIDTA) intelligence unit located at 801 W Michigan St. Milwaukee, WI 53233 for a Cellebrite extraction.

36. On October 30, 2020, a Cellebrite extraction of Suspect 1's cell phone was completed by North Central HIDTA Criminal Intelligence Analysts. Tens of thousands of files were found during the extraction. During the analysis of the files, it was discovered that the device's number is 773-297-7025. It was also discovered that the email address **earlcunningham90@gmail.com** is the primary email account associated with the device. Additionally, contents of the phone revealed that its owner often refers to himself as "Byrd Gezzy," with an associated email address of **byrdthroop@gmail.com**. According to the extraction files, between September 3, 2020 and October 25, 2020, there were 11 text messages referencing the assault of the postal worker. Additionally, on September 3 and 4, 2020 (the day and the day after Suspect 1 was pulled over by Inspectors and questioned about the assault), the device was used to complete internet searches for a web page on criminaldefenselawyer.com titled "I shoved someone and was charged with assault." Based on the above, there is reason to believe there may be location data, messages, photos, and internet search history related to the assault in either of both of Suspect 1's Google Accounts.

BACKGROUND CONCERNING GOOGLE

37. Google is an American multinational technology company that offers to the public, through its Google Accounts, a variety of online services, including email, cloud storage, digital

payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome and a free search engine called Google Search.

38. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device.

39. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the login username for access to the Google Account. Enterprises may also establish Google Accounts which can be accessed using an email address at the enterprise's domain (e.g. employee[@]company.com).

40. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

41. **GMAIL:** Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

42. **CONTACTS**: Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their mobile phone or device address book so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

43. **CALENDAR:** Google provides an appointment book for Google Accounts through Google Calendar. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device address book so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

44. **GOOGLE TASKS and GOOGLE KEEP:** Google also provides online to-do lists and notepads for Google Accounts. Google Tasks allows users to assign themselves tasks to be completed at scheduled times and marked complete when done. Google Keep allows users to create notes or lists. These notes can be shared with other users to edit. Users can set notifications at particular dates and times for both tasks and notes. Google preserves tasks and notes indefinitely, unless the user deletes them.

45. **WEB-BASED CHATS and MOBILE MESSAGING:** Google provides a number of direct messaging services accessible through a browser or mobile application, including Duo, Messages, Hangouts (Chat and Meet), and the now-retired Allo and Chat. These services enable real-time communications. Users can send and receive text messages, videos, photos, locations, links, and contacts from their Google Account using these services. Chat and Hangouts require or required the other user to also have a Google Account. Duo, Messages, and Allo do or did not. Google preserves messages sent through these services indefinitely, unless the user turns off the setting to save conversation history or deletes the message.

46. **GOOGLE DRIVE:** Google Drive is a cloud storage service automatically created for each Google Account. Users can store documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can also set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

47. **GOOGLE PHOTOS:** Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google

Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

48. **GOOGLE MAPS and GOOGLE TRIPS:** Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

49. **GOOGLE PLAY:** Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

50. **GOOGLE VOICE:** Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

51. **GOOGLE CHROME:** Google offers a free web browser service called Google Chrome, which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account.

52. **YOUTUBE:** Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, watch history, likes, comments, and change history to posted videos.

53. **INTEGRATION OF GOOGLE SERVICES:** Google integrates these various services to make it easier for Google Accounts to access the full Google suite of services. Users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

54. **SUBSCRIBER RECORDS:** When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

55. **ACCESS RECORDS:** Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

56. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

57. **BROWSING, SEARCH, and APPLICATION USE HISTORY:** Google collects and retains data about searches that users conduct within their own Google Account or using the Google Search service, including voice queries made to Google Assistant. Google also has the capacity to track the websites visited using its Google Chrome web browser service,

applications used by Android users, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google also collects and retains data about the voice queries made to its artificial intelligence-powered virtual assistant, Google Assistant, on Android devices and associated it with the registered Google Account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely, unless the user deletes them.

58. **LOCATION HISTORY:** Google collects and retains data about the location at which Google Account services are accessed from any mobile device regardless of service usage. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Google maintains these records indefinitely, unless the user deletes them.

59. Google also maintains records of the device characteristics of iPhones used to access Google services, including the make and model of the device. Depending on user settings,

those records may be associated with the Google Account logged into the service in use on the device. Google maintains these records indefinitely, unless the user deletes them.

60. In my training and experience, evidence of who was using a Google Account, and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. I also know, from my training and experience, that individuals who activate a Google Account for the purposes of only using a particular Google service (commonly email) will frequently generate records related to other services available with a Google Account, even inadvertently. This evidence may establish the "who, what, where, when, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

61. For example, the stored communications and files connected to a Google Account may provide direct evidence of the offense under investigation. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate about the offense under investigation.

62. In addition, the user's account activity, logs, stored electronic communications, location history, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a

relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). This sort of location data—in addition to the Location History information described above—is especially pertinent where, as here, there has been criminal activity at a specific location, and law enforcement must work to confirm the identity of individuals at that specific location.

63. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information on the Google Account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

64. Therefore, Google's servers are likely to contain stored electronic communications and information concerning Suspect 1 and his use of Google services. In my training and experience, such information may constitute evidence of the crime under investigation, including information that can be used to identify the account's user or users, their location(s) and activities at certain times relevant to the offense at issue, communications with others about the offense, and actions taken and research performed relating to the criminal offenses at issue.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

65. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

66. Based on the forgoing, I request that the Court issue the proposed search warrant.

67. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information which is associated with email addresses earlcunningham90@gmail.com and byrdthroop@gmail.com, which is stored at premises owned, maintained, controlled, or operated by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the "Provider"):

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any information that has been deleted but is still available to the provider, the Provider is required to disclose the following information to the government for the accounts listed in Attachment A for the time period of August 31, 2020 through October 27, 2020:

- **SUBSCRIBER AND ACCESS RECORDS:** All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, the date on which the account was created, the length of service, account status, alternative email addresses provided during registration, methods of connecting, log files, and subscriber change history;

- **LOCATION HISTORY:** All records indicating the location at which the account was active, such as Location History and Web & App Activity, including: GPS data; cell site/cell tower information; IP addresses; information associated with each location record, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car); and associated logs and user settings, including Timeline access logs and change history;

- **GOOGLE PHOTOS:** The contents of all media associated with the account in Google Photos, including deleted records; the creation and change history of each record; and any location, device, or third-party application data associated with each record;

- **BROWSING and SEARCH HISTORY:** All Internet search and browsing history, including search terms typed into the Google Chrome address bar or Google search bar;

- **MOBILE MESSAGING:** The contents of all messages associated with the account, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication; associated telephone numbers, including SMS recovery numbers; and usernames and other identifiers.

The Provider is hereby ordered to disclose the above information to the Government within 30 days of the Provider's receipt of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of the violation of Title 18, United States Code, Section 111 (assaulting a federal employee) for the accounts listed in Attachment A. This includes information pertaining to the following matters:

a) The identity of the person(s) who created or used the account;

b) Information indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

c) Evidence of the crime under investigation, including photographs of the victim;

d) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation, including internet searches about the crime and communications with others about the crime;

e) Information that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Postal Inspector may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.